



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/774,429	01/30/2001	Frederick William Strahm	10559/340001/P9885	3489
20985	7590	03/15/2004	EXAMINER	
FISH & RICHARDSON, PC 12390 EL CAMINO REAL SAN DIEGO, CA 92130-2081			HAMILTON, MONPLAISIR G	
		ART UNIT		PAPER NUMBER
		2172		9
DATE MAILED: 03/15/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	09/774,429	Applicant(s)	STRAHM ET AL.
Examiner	Monplaisir G Hamilton	Art Unit	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 26 January 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-15 and 17-26 is/are pending in the application.
 - 4a) Of the above claim(s) 16 is cancelled.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-15 and 17-26 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____

DETAILED ACTION

1. The communication filed on 12/22/03 amended Claims 1-2, 6, 11-12, 15, and 17 and cancelled Claim 16. Claims 1-15 and 17-26 remain for examination.

Response to Arguments

2. Applicant's arguments with respect to Claims 1-15 and 17-26 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claims 15 and 23-24 are objected to because of the following informalities: the claimed "encryption procedure" lacks support in base Claim 11. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 17 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 17 recites "each additional mechanism configured to communicate with the classification

forwarding device to *encrypt the packet if the packet is encrypted* and associated with a known encryption-related key, and, if the classification parameter is available, to forward the packet based on the route for the traffic stream". Examiner maintains that the claimed encrypting of an encrypted packet is not disclosed in the specification. Appropriate correction is required. Examiner has interpreted the claimed encrypting to mean decrypting.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1-2, 4-7, 9-26 are rejected under 35 U.S.C. 102(a) as being anticipated by US 6157955 issued to Narad et al, herein referred to as Narad.

Referring to Claims 1, 6 and 11:

Narad discloses a method comprising: determining at a first classifying forwarding element if a classification parameter is available for Internet Protocol security (IPsec) traffic that indicates a route for the IPsec traffic and classifying said traffic if available (col 9, lines 5-11; col 9, lines 25-35);

if said classification parameter is not available, and the IPsec traffic is encrypted then decrypting traffic in a decrypting forwarding element after said traffic has passed through said classifying forwarding element (col 6, lines 60-65; col 8, lines 5-15; col 9, lines 4-10, 30-45), and determining the classification parameter for the IPsec traffic at the decrypting forwarding element (col 9, lines 3-50); and

forwarding the IPsec traffic based on the classification parameter (col 6, line 64-col 7, line 11; col 8, lines 3-20).

Referring to Claims 2 and 7:

Narad discloses the limitations of Claims 1 and 6 above. Narad further discloses receiving the IPsec traffic at the classifying forwarding element (col 9, lines 5-30).

Referring to Claims 4 and 9:

Narad discloses the limitations of Claims 1 and 6 above. Narad further discloses the IPsec traffic includes a data packet (col 9, lines 5-10).

Referring to Claims 5 and 10:

Narad discloses the limitations of Claims 1 and 6 above. Narad further discloses forwarding other IPsec traffic included in a traffic stream with the IPsec traffic based on the classification parameter (col 9, lines 25-40).

Referring to Claim 12:

Narad discloses the limitations of Claim 12 above. Narad further discloses a third mechanism configured to communicate with the classifying forwarding element and with the decryption forwarding element and to determine a classification parameter for the packet if a classification parameter is not available (col 9, lines 15-45).

Referring to Claim 13:

Narad discloses the limitations of Claim 12 above. Narad further discloses the second mechanism is also configured to forward the packet to the third mechanism if the packet is not associated with a known encryption-related key (col 7, lines 1-15; col 9, lines 5-45).

Referring to Claim 14:

Narad discloses the limitations of Claim 12 above. Narad further discloses the third mechanism is also configured to, after determining the classification parameter for the packet, forward the classification parameter to the first mechanism (col 6, line 60-col 7, line 15; col 9, lines 15-40).

Referring to Claim 15:

Narad discloses the limitations of Claim 12 above. Narad further discloses the third mechanism is also configured to, after determining the encryption-related key for the packet, forward the encryption-related key to the decryption forwarding element so that the decryption forwarding element can perform the encryption-related procedure (col 6, line 60-col 7, line 15; col 9, lines 5-15).

Referring to Claim 17:

Narad discloses the limitations of Claim 11 above. Narad further discloses a plurality of additional mechanisms, each additional mechanism configured to communicate with the classification forwarding device to encrypt the packet if the packet is encrypted and associated

with a known encryption-related key, and, if the classification parameter is available, to forward the packet based on the route for the traffic stream (col 9, lines 10-45).

Referring to Claim 18:

Narad discloses the limitations of Claim 11 above. Narad further discloses the packet includes an Internet Protocol security data packet (col 9; lines 5-14).

Referring to Claim 19:

Narad discloses the limitations of Claim 11 above. Narad further discloses the traffic stream includes a plurality of Internet Protocol security data packets (col 9, lines 5-14).

Referring to Claim 20:

Narad discloses the limitations of Claim 11 above. Narad further discloses the first mechanism is also configured to forward the packet to the second mechanism if the packet is encrypted (col 9, lines 1-20).

Referring to Claim 21:

Narad discloses the limitations of Claim 11 above. Narad further discloses the route for the traffic stream includes a route through a network (col 7, lines 5-15).

Referring to Claim 22:

Narad discloses the limitations of Claim 21 above. Narad further discloses the network includes an Internet (col 7, lines 5-15).

Referring to Claim 23:

Narad discloses the limitations of Claim 11 above. Narad further discloses the encryption procedure includes encrypting the packet (col 9, lines 5-20).

Referring to Claim 24:

Narad discloses the limitations of Claim 11 above. Narad further discloses the encryption procedure includes decrypting the packet (col 9, lines 5-20).

Referring to Claim 25:

Narad discloses the limitations of Claim 11 above. Narad further discloses another mechanism configured to receive the packet from the second mechanism and to forward the packet based on the route to an ultimate destination of the packet (col 8, lines 10-30).

Referring to Claim 26:

Narad discloses the limitations of Claim 11 above. Narad further discloses the first mechanism is also configured to route packets included in the traffic stream based on a load balancing scheme (col 1, lines 35-40; col 3, lines 45-50; col 6, lines 40-55).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 3 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6157955 issued to Narad et al, herein referred to as Narad in view US 6484257 issued to Ellis, herein referred to as Ellis.

Referring to Claims 3 and 8:

Narad discloses the limitations of Claims 1 and 6 above.

Narad does not explicitly disclose “the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic”.

Ellis discloses the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic (col 3, lines 15-25).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Narad such that the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic. One of ordinary skill in the art would have been motivated to do this because it would allow the crypto module to identify the key needed to decrypt the packet (Ellis col 3, lines 15-25).

Prior Art

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 20030191848 issued to Hesselink, Lambertus et al. Hesselink discloses systems and methods for remote access of network-enabled devices that provide seamless, firewall-compliant connectivity between multiple users and multiple devices, that allow collaborative operations by multiple users of remote devices, that allow point to multipoint control of multiple devices and which allow rapid, secure transmission of data between remote users and devices. In general terms, the system includes at least one connection server, and at least two computers operatively coupled to the connection server via a public or global network. In an example where at least one client computer is operatively connected to at least one network-enabled device through a connection server via the public or global network, the connection server is configured to route control instructions from the client to the network-enabled device, and route data from the network-enabled device to the client.

US 20020062344 issued to Ylonen, Tatu et al. Ylonen discloses data packets are communicated between a transmitting virtual router in a transmitting computer device and a receiving virtual router in a receiving computer device. A security association is established for the secure transmission of data packets between the transmitting computer device and the receiving computer device. The transmitting virtual router and the receiving virtual router are identified within said security association. In the transmitting computer device, the security

association for processing a data packet coming from the transmitting virtual router is selected on the basis of the identification of the transmitting virtual router within the security association. In the receiving computer device, the security association for processing a data packet coming from the transmitting computer device is selected on the basis of values contained within the data packet. In the receiving computer device, the data packet processed within the security association is directed to the receiving virtual router on the basis of the identification of the receiving virtual router within the security association.

US 6578084 issued to Moberg, Kenneth A. et al. Moberg discloses a method for processing packets in a router includes specifying operations on packets as chains of processing elements. Each chain is uniquely associated with one interface/protocol pair, and each processing element performs at least one function on a packet. An incoming packet is received, and processed, first by a demultiplexor element which determines the protocol of the next higher level used by the packet. Then, the packet is processed by the elements of a decapsulation chain associated with the interface on which the packet was received, and by the elements of an encapsulation chain associated with the interface on which the packet is to be transmitted. The demultiplexor element or operation passes the packet on to a decapsulation chain associated with the protocol and with the incoming interface, depending on protocol information contained in the incoming packet. Decapsulation and encapsulation chains can be built dynamically, by inserting new and removing old elements as necessary as new protocols are developed and new features added. A chain walker walks through the chains, passing the processed packet to each element in a chain, until either the end of the chain is reached and

processing is complete, or until the packet is dropped because no function can process it, or because a packet is processed by an outside process or by hardware, which may optionally stop the chain walk. A chain walk may be temporarily halted, or may be terminated. If temporarily halted, the chain walk can be resumed at any element in the chain, depending on the packet's requirements. A chain walk can also begin at any element in a chain.

Final Rejection

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

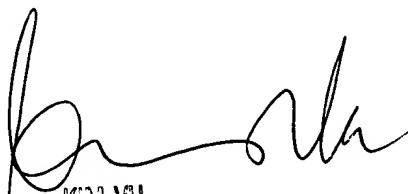
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monplaisir G Hamilton whose telephone number is (703) 305-5116. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Monplaisir Hamilton



KIM YU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100